DevSecOps Certified Professional Roadmap for Software Security Beginners

Introduction

Modern software teams are under constant pressure to release applications quickly. At the same time, they must protect data, reduce vulnerabilities, and maintain stable systems.This is where DevSecOps becomes important.DevSecOps brings security into the complete software delivery process. Instead of checking security only before release, teams include it during planning, development, testing, deployment, and monitoring.The DevSecOps Certified Professional (DSOCP) certification helps professionals understand how to build this security-first delivery approach.

Certification Overview

Category	Information
Certification name	DevSecOps Certified Professional
Short name	DSOCP
Provider	DevOpsSchool
Track	DevSecOps and Secure Software Delivery
Level	Professional
Suitable for	Developers, DevOps engineers, cloud engineers, security professionals, SREs, and managers
Recommended background	Basic understanding of Linux, Git, cloud, CI/CD, networking, and containers
Main skills	Pipeline security, cloud protection, container security, Kubernetes security, security testing, secrets management, and monitoring
Learning order	DevOps basics → Linux and Git → CI/CD → cloud → containers → security automation

What Is DSOCP?

DSOCP is a professional certification focused on securing modern software engineering practices.It teaches learners how to introduce security controls into applications, pipelines, infrastructure, containers, cloud platforms, and production environments.The certification is useful for professionals who want to move beyond basic DevOps and understand how secure delivery works in real organizations.

Who Should Consider This Certification?

DSOCP can be valuable for professionals working in technical and leadership roles.

It is suitable for:

- Software developers
- DevOps engineers
- Security engineers
- Cloud professionals
- Platform engineers
- Site reliability engineers
- System administrators
- Engineering managers
- Technical leads

Developers can learn how to identify security issues earlier. DevOps engineers can secure automation pipelines. Managers can understand how to create a practical DevSecOps roadmap.

Key Skills Covered

The certification helps learners develop skills in several important areas.

Secure Application Development

You learn how security risks can enter an application and how development teams can detect them early.

Important areas include:

- Secure coding awareness
- Threat modelling
- Code vulnerability scanning
- Dependency analysis
- Application security testing
- Secret detection

CI/CD Pipeline Protection

Modern pipelines contain source code, credentials, build tools, and deployment permissions. Protecting them is a major DevSecOps responsibility.

You learn about:

- Secure pipeline design
- Automated security testing
- Access control
- Credential protection

- Security approval gates
- Artifact verification

Cloud and Infrastructure Security

Cloud resources can become vulnerable because of incorrect permissions and insecure configurations.

DSOCP introduces:

- Identity and access management
- Least-privilege access
- Secure infrastructure as code
- Cloud logging
- Network protection
- Configuration scanning

Container and Kubernetes Security

Containers and Kubernetes are commonly used in modern application delivery.

The certification helps learners understand:

- Secure container images
- Image vulnerability scanning
- Kubernetes access control
- Network policies
- Admission policies
- Runtime protection
- Secrets handling

Monitoring and Incident Management

Security does not stop after deployment.

Learners also explore:

- Security monitoring
- Log analysis
- Alert management
- Runtime detection
- Incident response
- Security dashboards

Practical Projects You Should Build

A good DevSecOps professional should be able to apply knowledge through projects.

After preparation, you should be able to:

- Build a CI/CD pipeline with automated security checks
- Scan source code for vulnerabilities
- Detect exposed passwords and API keys
- Scan open-source dependencies
- Create a secure Docker image
- Check container images before deployment
- Protect cloud infrastructure using security policies
- Scan Terraform configurations
- Configure Kubernetes permissions
- Apply network policies
- Generate a software bill of materials
- Monitor suspicious runtime activity
- Create security alerts and dashboards
- Document a complete DevSecOps workflow

These projects can also strengthen your technical portfolio.

Preparation Options

7–14 Day Plan

This plan is best for experienced professionals.

Focus on:

- DevSecOps concepts
- CI/CD security
- SAST, DAST, and dependency scanning
- Docker and Kubernetes security
- Cloud identity
- Infrastructure scanning
- Monitoring and incident response

Build one complete project that connects code scanning, container security, and deployment controls.

30-Day Plan

This plan is suitable for working professionals.

Week 1: Review Linux, Git, networking, and DevOps concepts.

Week 2: Learn pipeline security, code scanning, dependency checks, and secret management.

Week 3: Practise Docker, cloud security, Terraform, and Kubernetes.

Week 4: Focus on monitoring, runtime protection, revision, and one final project.

60-Day Plan

This plan is recommended for beginners.

Use the first 15 days to understand Linux, Git, networking, cloud, and scripting.

Spend the next 15 days learning CI/CD, Docker, Terraform, and Kubernetes.

Use another 15 days for security testing, threat modelling, cloud security, and container protection.

Spend the final 15 days building projects, revising concepts, and improving documentation.

Common Learning Mistakes

Many learners focus too much on tools and ignore the larger process.

Avoid these mistakes:

- Memorising commands without understanding security risks
- Running scanners without analysing the results
- Treating DevSecOps as only a testing activity
- Keeping passwords inside code repositories
- Ignoring cloud permission issues
- Using vulnerable container images
- Skipping monitoring after deployment
- Blocking pipelines without proper planning
- Ignoring false positives
- Completing theory without practical labs

The goal is not to use the maximum number of tools. The goal is to build useful and reliable security controls.

Best Certification to Pursue Next

The right next certification depends on your career direction.

You may continue with:

- Advanced cloud security
- Kubernetes security
- Application security
- Site reliability engineering
- Platform engineering
- Infrastructure automation
- AIOps or MLOps
- FinOps
- Security governance

Choose a certification that supports your current role or your intended career path.

Choose Your Career Path

DevOps

Select this path when you want to focus on automation, cloud infrastructure, deployment pipelines, and platform operations.

DevSecOps

Choose this path when you want to specialise in security automation, application security, cloud protection, and secure delivery.

SRE

This path is useful for professionals interested in reliability, incident response, observability, availability, and production systems.

AIOps/MLOps

Choose this area when you want to work with AI-driven operations, machine learning platforms, automated monitoring, and model deployment.

DataOps

This path is suitable for professionals working with data pipelines, data quality, governance, automation, and analytics platforms.

FinOps

Choose FinOps when your role involves cloud spending, budgeting, cost visibility, resource optimisation, and governance.

Training and Certification Support Institutions

DevOpsSchool

DevOpsSchool provides the DSOCP certification and related professional training. It focuses on practical learning, tools, labs, and real-world implementation.

Cotocus

Cotocus supports learning and consulting in areas such as cloud, DevOps, automation, and digital engineering. It can help learners understand how technology practices are applied in business environments.

Scmgalaxy

Scmgalaxy offers technical knowledge related to software configuration management, CI/CD, DevOps tools, cloud, and automation.

BestDevOps

BestDevOps provides learning resources and information around DevOps technologies, practices, tools, and modern delivery methods.

DevSecOpsSchool

DevSecOpsSchool focuses on application security, secure pipelines, cloud protection, container security, and DevSecOps implementation.

SRESchool

SRESchool supports professionals who want to learn reliability engineering, monitoring, observability, incident handling, and production operations.

AIOpsSchool

AIOpsSchool focuses on intelligent IT operations, automation, analytics, monitoring, and AI-supported incident management.

DataOpsSchool

DataOpsSchool helps learners explore data pipeline automation, governance, data quality, platform management, and operational practices.

FinOpsSchool

FinOpsSchool focuses on cloud financial management, budgeting, resource optimisation, cost accountability, and cloud governance.

Conclusion

The DevSecOps Certified Professional certification is a useful learning path for professionals who want to combine software delivery with security.It helps learners understand how security can be built into source code, CI/CD pipelines, cloud resources, containers, Kubernetes, and production systems.The certification can support career growth in DevOps, DevSecOps, SRE, cloud security, platform engineering, DataOps, AIOps, MLOps, and FinOps.The best results come from combining certification study with hands-on projects. A professional who can design, implement, monitor, and explain secure delivery practices will be more valuable than someone who only understands the theory.